REMARKS

Background

In the Final Office Action of August 3, 2005, the Patent Office examined claims 2-67, claims 1 and 68-87 having already been withdrawn from consideration by Applicant's previous election.

The Patent Office rejected claims 2-21, 23, 24, 29-33, and 38 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,671,279 issued to Elgamal. Claims 2-33 and 37-67 were further rejected by the Patent Office under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,213,391 issued to Lewis in view of U.S. Patent No. 6,061,799 issued to Eldridge, et al. Claims 34-36 were deemed to contain allowable subject matter if rewritten in independent format or made to depend from an otherwise allowable independent claim.

With the present amendment, claims 1-87 have now been cancelled and new claims 88-146 have been presented for consideration. Dependent claims 89-146 are substantially the same as previous dependent claims 3-67. The only independent claim 88 is a replacement to the previously-pending independent claim 2. Claim 88 re-presents the subject matter of now-cancelled claim 2 to more clearly point out and claim the invention of this application. It is respectfully submitted that no new matter has been introduced by the present amendment and that no new search is required of the Examiner by the presentation of new claims 88-146.

Response to Rejections under 35 U.S.C. §§102(b) and 103(a) and Reasons Why New Claims 88-146 are Allowable

Elgamal

The patent to Elgamal appears to describe, generally, a protocol to secure a courier electronic payment system that provides customers, merchants, and banks with a system for credit card payment services. The system, as disclosed, regulates the

relationship between a customer, a merchant, and an acquiring bank in order to implement credit card purchases securely over a network. This entire system requires and relies upon "digital certificates" to ensure the link between each party's respective public key and their identity. See columns 15-20 of Elgamal (entire protocol requires a third party digital certificate to authenticate the "link" between each public key and the entity to which it belongs).

New independent claim 88 covers a method of authenticating an account holder by an account authority, comprising the steps of: (i) as part of setup of an account of the account holder: (a) recording information pertaining to the account in a database of the account authority, the information not including any third party digital certificates; (b) assigning a respective unique identifier to the account, such that the recorded information pertaining to the account is retrievable from the database based on its unique identifier; (c) associating a public key of a public-private key pair of the account holder with the unique identifier such that the public key is retrievable based on the unique identifier, wherein the private key is not stored in the database of the account authority but rather stored securely within a device of the account holder, the device being adapted to generate digital signatures using the private key stored therein; and (ii) thereafter: (d) receiving, by the account authority, an electronic communication containing the unique identifier, a message regarding the account, and a digital signature of the message; (e) retrieving from the database the associated public key based on the received unique identifier; (f) authenticating the digital signature using the associated public key to confirm that the digital signature was generated using the private key stored in the device and to confirm the integrity of the message; and (g) if the digital signature and message successfully authenticate using the associated public key, acting upon the message regarding the account without also requiring any third party digital certificate to authenticate the link between the public key and the account holder. It is respectfully submitted that the present invention covers a method and system in which an account authority associates an account holder's public key with an account without the need for

or use of third party digital certificates. There is no need for such digital certificates in this invention because the account authority, which set up the account for the account holder in the first place, is the same party that is later receiving and authenticating an electronic communication digitally signed using the corresponding private key. No third party digital certificates are required to "link" the account holder with the public key because such linkage has already been done directly by the account authority at a time prior to the electronic communication.

Thus, Elgamal does not teach each and every element of the limitations of independent claim 88.

Lewis

Lewis was cited as a primary reference in the rejection of now cancelled claims 2—67 under 35 U.S.C. §103(a). Lewis appears to describe a portable device for use in confirming personal identification of the user of the device based upon distinctive characteristics of the user. As shown in FIG. 1 of Lewis, such device 1 stores or pre-stores user profiles in (database) storage 6. Such user profiles include distinctive characteristics of the user, such as digitized biometric information. Suspect user identification information is input into the device at input 12,14. If necessary, such suspect user identification information is digitized and then compared with the pre-stored user profiles from storage 6. If there is a match, a positive ID signal is generated and sent to output 10. If there is not a match, a negative ID signal is generated and sent to output 10. As a back-up, the digitized suspect user identification information 4 is also converted into a suitable code by means of code generator 5 and such code is sent to output 11. This generated code is useful as a "secondary, or alternative method of determining identification and authorization." (col. 9, ll. 3-5). However, it is necessary for the recipient of the signal from output 11 to have access to or prior knowledge of the user's profile and the technique or algorithm used by code generator 6 in order to determine independently whether there is a match, FIG. 2 appears to describe a similar but slightly

different embodiment compared to FIG. 1. In FIG. 2, the signals at outputs 30, 29 are encrypted to prevent interception of such information as it is transmitted to the recipient.

Nothing in Lewis teaches, discloses, or suggests a method of authenticating an account holder by an account authority, comprising the steps of: (i) as part of setup of an account of the account holder: (a) recording information pertaining to the account in a database of the account authority, the information not including any third party digital certificates; (b) assigning a respective unique identifier to the account, such that the recorded information pertaining to the account is retrievable from the database based on its unique identifier; (c) associating a public key of a public-private key pair of the account holder with the unique identifier such that the public key is retrievable based on the unique identifier, wherein the private key is not stored in the database of the account authority but rather stored securely within a device of the account holder, the device being adapted to generate digital signatures using the private key stored therein; and (ii) thereafter: (d) receiving, by the account authority, an electronic communication containing the unique identifier, a message regarding the account, and a digital signature of the message; (e) retrieving from the database the associated public key based on the received unique identifier; (f) authenticating the digital signature using the associated public key to confirm that the digital signature was generated using the private key stored in the device and to confirm the integrity of the message; and (g) if the digital signature and message successfully authenticate using the associated public key, acting upon the message regarding the account without also requiring any third party digital certificate to authenticate the link between the public key and the account holder.

It is respectfully submitted that Lewis, which is directed to a portable device that contains information about a user of the device and which authenticates the user of the device by comparing information input into the device with information pre-stored in the device has limited-to-no relevance and applicability to the method of the present invention, as set forth in independent claim 88.

Eldridge

The second, supporting reference relied upon by the Patent Office, Eldridge, appears to describe a dual shared-secret authentication system useful for authenticating a client process to a server process. The client process uses a portable medium or device to store both current and past passwords of the client process. Each password (current and past) on the portable medium has associated with it a key (e.g., a public-private key pair or just a public key) and a key ID wherein the key and corresponding key ID are both derived from the client-chosen password. The client process (portable medium/device) also has an associated client ID for identifying itself to the server process. The server process also possesses the same key-key ID pairs, as well as the associated client ID (see, e.g., col. 7, ll. 64-col. 8, ll. 12).

To authenticate, as shown in FIG. 5 of Eldridge (col. 7), the client process first provides its client ID to the server process (col. 7, ll. 22-24). The server process then retrieves the associated key ID and provides it to the client process (col. 7, ll. 24-30). The client process uses this key ID to identify the corresponding key and provides such key back to the server process (col. 7, ll. 30-43). The server process then generates a new key ID from the key received from the client process and compares this new key ID with the key ID it originally sent. If these match, then the client process is authenticated (col. 7, ll. 43-48). In an alternative, more simplistic, and less reliable embodiment, as shown in FIG. 7 of Eldridge (col. 9), the server process extracts both the client ID and key ID from the portable medium (col. 9, ll. 40-50). The server process uses the client ID to identify the corresponding key IDs previously stored in its own database. If there is a match, then the client process is authenticated.

It is also respectfully submitted that Eldridge does not assist in making Lewis a more relevant reference. Further, nothing in Eldridge teaches, discloses, or suggests a method of authenticating an account holder by an account authority, comprising the steps of: (i) as part of setup of an account of the account holder: (a) recording information pertaining to the account in a database of the account authority, the information not

including any third party digital certificates; (b) assigning a respective unique identifier to the account, such that the recorded information pertaining to the account is retrievable from the database based on its unique identifier; (c) associating a public key of a public-private key pair of the account holder with the unique identifier such that the public key is retrievable based on the unique identifier, wherein the private key is not stored in the database of the account authority but rather stored securely within a device of the account holder, the device being adapted to generate digital signatures using the private key stored therein; and (ii) thereafter: (d) receiving, by the account authority, an electronic communication containing the unique identifier, a message regarding the account, and a digital signature of the message; (e) retrieving from the database the associated public key based on the received unique identifier; (f) authenticating the digital signature using the associated public key to confirm that the digital signature was generated using the private key stored in the device and to confirm the integrity of the message; and (g) if the digital signature and message successfully authenticate using the associated public key, acting upon the message regarding the account without also requiring any third party digital certificate to authenticate the link between the public key and the account holder, as set forth in independent claim 88.

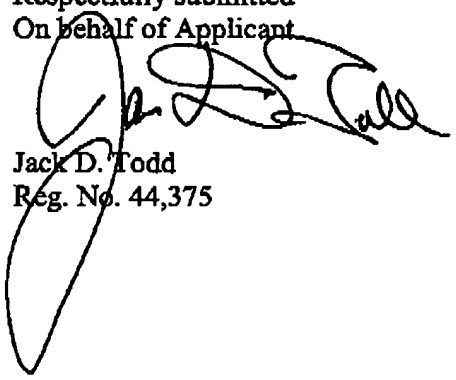
Dependent Claims

Further, because the only pending independent claim 88 is believed to stand in condition for allowance, Applicant submits that the dependent claims 89-146 similarly are allowable. Applicant nevertheless respectfully submits that each of these dependent claims is allowable based on the additional recitation of such dependent claim, and Applicant requests consideration thereof as necessary. Applicant further does not acquiesce in the rejections of these dependent claims, but Applicant does not *per se* address each such rejection, as Applicant believes such rejections are moot in view of the foregoing remarks.

Conclusion

In view of the foregoing amendments and remarks, the enclosed terminal disclaimers, and associated fees, Applicant submits that the present claims now stand in condition for allowance, and Applicant respectfully requests notice of the same. It furthermore is respectfully requested that the Examiner contact the undersigned if any further action is deemed necessary in order to gain allowance of the present application, and if such further action may be accomplished through action by the Examiner.

Respectfully submitted
On behalf of Applicant



Jack D. Todd
Reg. No. 44,375

MORRIS, MANNING & MARTIN, LLP

3343 Peachtree Road, N.E.
1600 Atlanta Financial Center
Atlanta, Georgia 30326
(404) 233-7000 (main)
(404) 504-7674 (direct)
Customer No. 24728